3. Passive Reconnaissance

🌐 DNS, Reconnaissance & Domain Intelligence

🕵️ 1. What Can We Learn About a Server?

From a server, we can extract critical information such as:

- **IP address and geographic location**
- **Operating system and version** (via banner grabbing, OS fingerprinting)
- **Open ports and running services**
- **Server software and versions** (e.g., Apache 2.4.41)
- **DNS records and domain info**
- **SSL/TLS certificates** and cryptographic details
- **Security misconfigurations or vulnerabilities**
- **Subdomains and associated infrastructure**

⚠️ This info helps assess attack surfaces or verify defenses.

🖥️ 2. What is a DNS Server?

DNS (Domain Name System) server translates **human-readable domain names** (like `www.holbertonschool.com`) into **IP addresses** (e.g., `192.0.2.1`).

- Acts like the **"phone book" of the internet**.
- Resolves queries by looking up various DNS records.
- Can be **authoritative** (for domains it manages) or **recursive** (resolves queries by querying other DNS servers).

🌐 3. What Happens When We Type www.holbertonschool.com and Press ENTER?

1. **Browser checks cache** for DNS record. If not found, it queries the local DNS resolver (ISP or corporate).
2. Resolver queries **root DNS servers** to find the **TLD (Top-Level Domain)** servers for `.com`.
3. Resolver queries `.com` TLD servers for authoritative DNS server for `holbertonschool.com`.
4. Resolver queries authoritative DNS server for `www.holbertonschool.com` to get the IP.
5. IP address returned to the browser.
6. Browser initiates a **TCP connection** (usually on port 80 or 443).

7. Browser sends an **HTTP/HTTPS request** to the server.
8. Server responds with website content.

🔎 4. How Can We Find the Owner Information for a Domain Name?

Use **WHOIS** lookup to retrieve domain registration info:

- Owner's name, organization, contact emails, phone numbers.
- Registrar company.
- Creation, update, and expiry dates.
- Name servers in use.

WHOIS can be queried via:

- Command line:

```
whois holbertonschool.com
```

- Online services like `whois.domaintools.com`.

⚠️ Some domains use **privacy protection** or **GDPR** masking.

🛠️ 5. What is dig?

`dig` (Domain Information Groper) is a **command-line DNS lookup tool** used to query DNS servers for records.

Example:

```
dig www.holbertonschool.com A
```

Can query for any DNS record type (`A`, `MX`, `TXT`, `NS`, etc.), specify DNS servers, and output detailed info for analysis.

🛠️ 6. What is nslookup?

`nslookup` is an older DNS lookup utility with interactive and non-interactive modes.

Example:

```
nslookup www.holbertonschool.com
```

Provides DNS info like IPs, name servers, and supports debugging queries.

`dig` is generally preferred due to more detailed output.

📜 7. What Are the Different Types of DNS RECORDS?

Record Type	Purpose
A	IPv4 address of a domain or hostname.
AAAA	IPv6 address.
CNAME	Canonical name (alias) of another domain.
MX	Mail exchange servers for email routing.
NS	Name servers authoritative for the domain.
TXT	Arbitrary text info (used for SPF, DKIM, verification).
PTR	Reverse DNS lookup (IP → domain).
SOA	Start of Authority, zone info and TTL settings.
SRV	Service records (e.g., VoIP, XMPP).

🕵️‍♂️ 8. What is DNS Dumpster?

DNS Dumpster is a **free online tool** for gathering DNS information and mapping the attack surface:

- Enumerates DNS records for a domain.
- Finds subdomains, mail servers, name servers.
- Visualizes DNS infrastructure with **network maps**.
- Useful for **passive reconnaissance**.

https://dnsdumpster.com

🚀 9. What is Shodan.io?

Shodan is a **search engine for internet-connected devices** (IoT, servers, webcams, routers).

- Can find devices by IP, location, software, vulnerabilities.
- Useful for discovering exposed services or devices.
- Powerful for **attack surface discovery** and monitoring.

🔍 10. How Can We Find Subdomains?

Methods to find subdomains:

- **Passive reconnaissance**: tools like `subfinder`, `Amass`, `crt.sh` (certificate transparency logs), Google dorks, and online services like VirusTotal.
- **Brute force**: using wordlists with tools like `dnsenum`, `dnsrecon`, or `massdns`.
- **DNS zone transfers** (rarely allowed, but possible).

- Use OSINT and bug bounty platforms.

🛠️ 11. What is subfinder?

`subfinder` is a **fast passive subdomain discovery tool** that aggregates data from multiple public sources.

- Does **not** perform brute forcing by default.
- Sources include APIs like VirusTotal, CertSpotter, etc.
- Can be combined with brute force tools for thorough enumeration.

⚔️ 12. What is the Difference Between Active and Passive Reconnaissance?

Aspect	Active Reconnaissance	Passive Reconnaissance
Interaction	Direct interaction with target systems/networks.	No direct interaction; uses public/open sources.
Examples	Port scanning, banner grabbing, ping sweeps.	WHOIS, DNS queries, web scraping, OSINT.
Risk	Detectable, may trigger alarms or alerts.	Usually stealthy and hard to detect.
Purpose	Gather detailed info, confirm vulnerabilities.	Collect broad info for initial footprinting.
